

Digitalising Energy: Navigating The Protection of Consumer Rights and Privacy in Malaysia

Nurdina Sofiya Binti Zaini¹, Nurul Hannah Binti Mohd Haris¹, Nur Amni Syamim Binti Faizul¹, Siti Mariam Mellisa Binti Abdullah^{2*}, Mohd Haris Bin Abdul Rani³

¹Research Associate, Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

² Senior Lecturer, Universiti Teknologi MARA Cawangan Selangor, Kampus Dengkil, 43800 Dengkil, Selangor, Malaysia

³ Senior Lecturer, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100801048>

Received: 10 September 2026; Accepted: 15 September 2026; Published: 23 September 2026

ABSTRACT

The digitalisation of the energy sector, driven by technologies such as smart infrastructure, Internet of Things (IoT) devices, and AI-powered energy management systems, has transformed the way consumers interact with energy services. While these technologies offer greater efficiency and convenience, they also raise important legal concerns regarding consumer data privacy, transparency, informed consent, and data security. This article examines the legal implications of digital energy technologies, with particular attention to how energy providers collect, process, and use consumer data and the risks associated with data security breaches. Using doctrinal and comparative legal methods, the article analyses Malaysia's Personal Data Protection Act 2010 (PDPA), including the reforms introduced by the Personal Data Protection (Amendment) Act 2024, against the European Union's General Data Protection Regulation (GDPR). The analysis assesses whether Malaysia's post-amendment framework adequately protects consumers against the privacy risks associated with increasingly data-driven energy services. Although the recent amendments have strengthened Malaysia's data protection framework, several regulatory concerns remain, particularly in relation to transparency, consumer control over personal data, and the governance of emerging digital technologies. The article concludes that further sector-specific safeguards and effective enforcement mechanisms are necessary to strengthen consumer autonomy, privacy, and data security in Malaysia's digital energy sector.

Keywords: Consumer data privacy; Digital energy technologies; Personal Data Protection Act 2010 (PDPA); General Data Protection Regulation (GDPR); Consumer protection; Data security

INTRODUCTION

The rapid development of digital technologies has transformed various sectors of the economy, including the energy sector. Energy providers increasingly rely on smart infrastructure, Internet of Things (IoT) devices, and AI-powered energy management systems to collect, analyse, and utilise data more effectively (Ahmad & Zhang, 2021). Digitalisation can improve energy efficiency and contribute to more sustainable and cost-effective energy systems (Husaini & Lean, 2022). However, the growing use of data-driven technologies also raises important legal concerns, particularly regarding consumer data protection, transparency, informed consent, and privacy (Montalbano, 2021). As energy services become increasingly digitalised, maintaining a balance between technological efficiency and consumer privacy has become an important regulatory challenge (Quach et al., 2022).

Digital technologies have also changed the way consumers interact with energy services. Through smart meters, digital applications, automation, and connected devices, consumers can monitor and manage their energy consumption in real time (Muralidhara et al., 2020). At the same time, these technologies enable energy providers to collect increasingly detailed information about consumers, including their energy-use patterns, behaviours, and preferences (Jakobi et al., 2019). Although such data may improve the efficiency and personalisation of energy services, its extensive collection and processing create

potential risks to consumer privacy and data protection (Wang et al., 2021). These concerns become particularly important when consumers have limited knowledge of how their information is collected, processed, shared, or retained.

Consumer privacy has therefore become an increasingly important issue in the digital energy environment. As data-collection technologies become more sophisticated, consumers may have limited practical control over how their personal information is processed (Bélanger & Crossler, 2011). Unlike traditional energy systems, digital energy technologies can generate detailed and continuous information about household energy consumption and consumer behaviour. Smart-meter data, for example, may reveal patterns that extend beyond basic billing information and provide insights into household activities and consumption practices (Jakobi et al., 2019). Without adequate legal safeguards, such information may potentially be used for behavioural profiling, targeted marketing, or other secondary purposes that consumers may not reasonably anticipate (Strycharz & Duivenvoorde, 2021). This highlights the importance of an effective regulatory framework that protects consumer rights while allowing the benefits of digital energy technologies to develop.

Data security is equally important because digital energy systems are increasingly interconnected. Security breaches or unauthorised access may expose personal consumer information and potentially lead to identity theft, financial loss, disruption of services, and loss of consumer trust (Abrahams et al., 2024; George et al., 2024). The interconnected nature of digital energy infrastructure also means that vulnerabilities in one part of the system may create wider consequences for consumers and service providers. Accordingly, data protection in the digital energy sector requires consideration of both privacy and security, together with appropriate legal and regulatory safeguards (Heffron et al., 2018).

The European Union's General Data Protection Regulation (GDPR) is widely recognised as an influential framework for personal data protection. It provides detailed requirements relating to transparency, lawful processing, data-subject rights, data portability, erasure, accountability, and regulatory enforcement. Malaysia primarily regulates personal data processing in commercial transactions through the Personal Data Protection Act 2010 (PDPA). The Malaysian framework has recently undergone significant reform through the Personal Data Protection (Amendment) Act 2024, which introduced several important measures, including data breach notification requirements, provisions concerning Data Protection Officers, enhanced data portability rights, and increased penalties for certain contraventions.

These amendments have strengthened Malaysia's data protection framework and narrowed some of the earlier differences between the PDPA and international data protection standards. Nevertheless, the increasing use of smart meters, IoT devices, AI-based energy management systems, automated processing, and interconnected digital platforms raises questions about whether the existing framework adequately addresses the distinctive privacy risks associated with digital energy services. The issue is therefore no longer simply whether Malaysia provides particular data-protection rights, but whether the scope, implementation, and enforcement of those protections are sufficient to safeguard consumers in an increasingly data-driven energy environment.

Against this background, this article employs doctrinal and comparative legal methods to examine the protection of consumer data and privacy within Malaysia's digital energy sector. It analyses Malaysia's PDPA, including the reforms introduced by the Personal Data Protection (Amendment) Act 2024, in comparison with the GDPR. The analysis focuses particularly on consent and transparency, data-subject rights, data portability, data security, regulatory enforcement, and emerging concerns associated with digital energy technologies. The article seeks to identify the remaining regulatory gaps in Malaysia's post-amendment framework and considers how consumer protection may be strengthened while supporting the continued development of digital energy services.

Accordingly, the study is organised around three research questions: (RQ1) To what extent has the Personal Data Protection (Amendment) Act 2024 strengthened the protection of consumer data in Malaysia's digital energy sector? (RQ2) How does Malaysia's post-amendment PDPA compare with the GDPR in relation to the principal data-protection issues arising from digital energy technologies? (RQ3) What legal and regulatory gaps remain in Malaysia's framework, and which regulatory mechanisms are most appropriate for strengthening the protection of digital energy consumers?

LITERATURE REVIEW

Digitalisation and the Transformation of Energy Services

Digitalisation refers to the increasing integration of digital technologies into organisational processes, communication, service

delivery, and interactions with users. It has transformed the way organisations collect, process, store, and use information across various sectors (Verhoef et al., 2021). Technologies such as artificial intelligence (AI), the Internet of Things (IoT), cloud computing, automation, and data analytics have further accelerated this transformation by enabling real-time data processing and increasingly interconnected services.

Within the energy sector, digitalisation has changed the way energy is produced, distributed, monitored, and consumed. Smart meters, IoT-enabled devices, digital platforms, and automated energy management systems allow energy providers to monitor consumption patterns and improve the efficiency of energy services. At the same time, these technologies enable consumers to access information about their energy consumption and make more informed decisions regarding energy use. Digitalisation therefore creates opportunities to improve efficiency and sustainability while encouraging greater consumer participation in energy management.

However, these developments also increase the amount and variety of consumer data collected by energy providers. Digital energy systems may continuously generate information concerning household energy consumption, behavioural patterns, device usage, and consumer preferences. Consequently, the benefits associated with digitalisation must be considered alongside concerns relating to data privacy, cybersecurity, transparency, and consumer control over personal information.

The Changing Role of Consumers in the Digital Energy Sector

Digitalisation has also transformed the traditional role of consumers. Consumers are no longer merely passive recipients of goods and services but increasingly participate in digital markets through online platforms, connected devices, and data-driven services. Businesses use technologies such as AI and big-data analytics to better understand consumer behaviour and develop more personalised products and services.

This transformation is particularly evident in the energy sector. Smart meters and IoT-enabled devices allow consumers to monitor and regulate their energy consumption in real time (Nageye et al., 2023). Renewable energy technologies have also contributed to the emergence of “prosumers”, who both produce and consume energy, particularly through technologies such as rooftop solar systems (Oprea & Băra, 2024). These developments give consumers a more active role within modern energy systems.

Nevertheless, increased participation in digital energy systems also creates new vulnerabilities. Consumers may not fully understand the extent to which their information is collected, analysed, retained, or shared with third parties. Detailed energy-consumption information may reveal patterns relating to household routines and behaviour. The growing reliance on consumer data therefore raises questions about transparency, meaningful consent, data security, and the extent to which consumers retain control over their personal information.

Consumer Welfare and Energy Justice

The protection of consumers in digital energy systems may also be considered through the broader principles of energy justice. Procedural justice emphasises fairness, transparency, participation, and inclusion in decision-making processes affecting energy consumers. From this perspective, consumers should receive sufficient information about how their personal data are collected and used and should have meaningful opportunities to exercise their rights over such information.

The principle of resilience is also relevant to increasingly interconnected energy systems. Digital energy infrastructure should be capable of withstanding and recovering from disruptions, including cyberattacks and data breaches. Resilience therefore extends beyond the operational reliability of energy services to include the protection of consumer information processed through digital infrastructure. Strong data-security practices and appropriate legal safeguards are consequently important both for maintaining reliable energy systems and for protecting consumer privacy. These considerations demonstrate that the digitalisation of the energy sector is not solely a technological issue. It also involves questions of consumer welfare, fairness, privacy, security, and regulatory accountability. An effective legal framework must therefore balance technological innovation and energy efficiency with adequate protection of consumer rights.

The Energy Sector in the Digital Era

The energy sector encompasses the production, distribution, supply, and consumption of energy from various sources, including conventional and renewable resources. Increasing digitalisation has added a significant data-driven dimension to

these activities. Smart grids, smart meters, connected devices, and AI-based energy management systems now form part of an increasingly interconnected energy infrastructure.

The use of these technologies creates substantial opportunities for more efficient energy management, but it also generates new regulatory challenges. Energy providers may process large quantities of personal and consumption-related data as part of billing, service delivery, system monitoring, forecasting, and customer support. As energy systems become increasingly dependent on digital technologies, the protection of this information becomes closely connected to both consumer privacy and the resilience of energy infrastructure.

Accordingly, the legal regulation of digital energy should address not only the reliability and efficiency of energy services but also the collection, processing, storage, disclosure, and security of consumer data. This relationship between technological innovation, energy services, and personal data protection provides the basis for examining the adequacy of Malaysia's legal framework in protecting consumers within the digital energy environment.

Protecting Information: Data Privacy and Security

The rapid development of technologies such as the Internet of Things (IoT), smart devices, cloud computing, and artificial intelligence has significantly increased the volume of data collected, stored, and processed by organisations (Bertino, 2016). As digital systems become increasingly interconnected, concerns regarding data privacy and security have also become more significant. Protecting personal information while ensuring that data can be securely stored, accessed, and processed is therefore an important challenge in the digital environment (Ke & Yongzhen, 2021).

Although data privacy and data security are closely related, they address different aspects of data protection. Data privacy focuses on how personal information is collected, processed, used, and disclosed, as well as the individual's ability to exercise control over such information. Data security, on the other hand, concerns the measures used to protect data from unauthorised access, loss, misuse, alteration, or disclosure (Anil et al., 2024; Fayayola et al., 2024). Together, privacy and security provide complementary safeguards for protecting personal information.

These concerns are particularly relevant as organisations increasingly rely on interconnected technologies that generate and process large quantities of information. Cyberattacks may exploit vulnerabilities in computer systems, networks, applications, and digital infrastructure to gain unauthorised access to sensitive information or disrupt operations (Ahmed & Ahmed, 2023; Cremer et al., 2022). Emerging technologies such as IoT and AI further complicate data governance because they enable data to be collected and analysed continuously and on a large scale (Hoang, 2024).

The risks associated with inadequate data privacy and security affect individuals, organisations, and governments. For individuals, effective privacy and security measures can reduce the risk of identity theft and misuse of personal information (Kavak, 2024). For organisations, appropriate data-security practices are important for maintaining consumer trust, complying with regulatory requirements, and reducing the financial and reputational consequences associated with data breaches. Governments and regulators similarly have an important role in ensuring that data-processing activities are conducted within an appropriate legal and regulatory framework.

These concerns are particularly significant in the digital energy sector, where smart meters, connected devices, and automated energy systems may continuously process information relating to household energy consumption. The interconnected nature of these systems means that weaknesses in data security may affect not only the confidentiality of consumer information but also trust in digital energy services. Consumer data protection should therefore be incorporated into the governance and design of digital energy systems rather than treated solely as a response to data breaches.

The principle of procedural justice further supports the need for transparent, inclusive, and fair processes when technological developments significantly affect consumers (Jenkins et al., 2016). In the context of digital energy systems, consumers should receive clear information about how their data are collected and used and should be given meaningful opportunities to exercise their rights. This is particularly important where consumers may have limited knowledge of smart-grid technologies or automated energy systems. Greater transparency and consumer participation may strengthen public trust while supporting the responsible adoption of digital energy technologies.

What Is the Personal Data Protection Act 2010?

The Personal Data Protection Act 2010 (PDPA) [Act 709] is Malaysia's principal legislation governing the processing of personal data in commercial transactions. Its primary objective is to regulate the processing of personal data and protect the interests of data subjects. The Act applies to persons who process, control, or authorise the processing of personal data in connection with commercial transactions, subject to its statutory scope and exemptions. In particular, the Federal and State Governments are excluded from its application.

A significant limitation of the statutory scope is that the PDPA does not apply to the Federal Government or State Governments. In the digital-energy context, this exclusion matters where personal or consumption-related data are processed by governmental bodies, public-sector programmes or public digital infrastructure. The consequence should not be overstated as an absence of all legal protection; rather, such processing falls outside the protections and enforcement architecture of the PDPA itself and may instead depend on other applicable public-law, administrative, cybersecurity or sectoral arrangements. As public and private actors increasingly collaborate in digital infrastructure, this distinction may also produce uneven protection depending on the identity of the entity processing the same or similar categories of consumer data.

The PDPA establishes seven fundamental principles governing the processing of personal data: the General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle, and Access Principle. Collectively, these principles regulate matters such as consent, notification of the purposes for which data are processed, disclosure of personal information, security safeguards, retention periods, accuracy of data, and individuals' ability to access and correct their personal information.

These principles are particularly relevant to the digital energy sector. Smart meters, mobile applications, connected devices, and digital energy-management systems may generate and process information capable of identifying individual consumers or revealing detailed patterns of household energy consumption. Where such personal data are processed in connection with commercial transactions, energy providers falling within the scope of the PDPA are required to comply with the applicable data-protection obligations. The Notice and Choice and Security Principles are especially significant because consumers should be informed about the processing of their information, while organisations must take appropriate measures to protect personal data from loss, misuse, modification, unauthorised access, or disclosure.

The regulation of personal data in the energy sector is further supported by sector-specific requirements. The Personal Data Protection Code of Practice for the Utilities Sector (Electricity) provides additional guidance concerning the processing of personal data within the electricity sector. Such sector-specific regulation is important because digital energy services increasingly involve continuous and potentially detailed data collection through smart meters and other connected technologies (Personal Data Protection Commissioner, 2016).

Legal Status and Adequacy of the Utilities Sector (Electricity) Code of Practice

The Utilities Sector (Electricity) Code of Practice should not be treated merely as informal guidance. It forms part of the sector-specific regulatory architecture developed under the Personal Data Protection Act 2010 (PDPA). The Code was developed pursuant to section 23(1)(b) of the PDPA and is intended to regulate the processing of personal data within the utilities (electricity) sector, protect the rights of data subjects, and provide an operational approach to the data-protection principles established under the Act (Personal Data Protection Commissioner [PDPC], 2016). Its legal significance therefore lies in providing sector-specific standards for entities within its scope, supplementing the general statutory framework with requirements adapted to electricity-sector processing activities.

The adequacy of the Code, however, must now be assessed against a substantially more data-intensive energy environment than existed when the earlier sectoral framework was developed. Smart meters, IoT-enabled devices, cloud services, AI-based energy-management systems, and data-sharing ecosystems can generate continuous and granular information capable of revealing household routines and behavioural patterns (Jakobi et al., 2019; Vigurs et al., 2021). The Code should therefore be reviewed and aligned with the amended PDPA, particularly in relation to data-breach notification, DPO responsibilities, data portability, privacy by design, impact assessment, automated decision-making, profiling, retention, secondary use, and third-party sharing. An updated enforceable sectoral code could provide greater regulatory specificity than general guidance alone while preserving flexibility for technological change.

Cross-border data transfers are another important consideration as energy providers increasingly use cloud services and interconnected digital platforms. Section 129 of the PDPA regulates the transfer of personal data outside Malaysia. The current framework requires data controllers to ensure that cross-border transfers comply with the statutory requirements and applicable safeguards. Malaysia has also issued specific guidance on cross-border transfers to clarify compliance with section 129 and assist data controllers in determining the applicable conditions for transfers outside Malaysia (Personal Data Protection Commissioner [PDPC], 2025a).

Strengthening the PDPA: The Personal Data Protection (Amendment) Act 2024

Malaysia significantly strengthened its personal data protection framework through the Personal Data Protection (Amendment) Act 2024 [Act A1727]. The amendments introduced important reforms to the PDPA and represent a substantial development in Malaysia's approach to data governance. Among the reforms are enhanced requirements concerning data security, data breach notification, the appointment of Data Protection Officers (DPOs), data portability, and increased penalties for certain contraventions. The terminology of the legislation was also modernised, including the replacement of the term "data user" with "data controller" (Personal Data Protection (Amendment) Act 2024).

Commencement and Operation of the 2024 Amendments

The 2024 amendments did not commence on a single date. Under the *Personal Data Protection (Amendment) Act 2024 (Appointment of Date of Coming into Operation)*, P.U. (B) 522, sections 7, 11, 13 and 14 came into operation on 1 January 2025; sections 2, 3, 4, 5, 8, 10 and 12 on 1 April 2025; and sections 6 and 9 on 1 June 2025. The staggered commencement is legally significant because the post-amendment framework became operational in phases rather than immediately upon enactment. By September 2026, all provisions specified in the commencement notification are in force. The analysis in this article therefore evaluates the PDPA as an operative post-amendment regime, while recognising that its implementation also depends on subsidiary instruments, Commissioner circulars, and regulatory guidance.

Operationally, the Personal Data Protection (Amendment) Act 2024 (Act A1727) introduced or strengthened several mechanisms relevant to data-intensive energy services, including the appointment of Data Protection Officers (DPOs), mandatory data-breach notification, data portability, and enhanced data-security obligations. Subsequent regulatory materials issued by the Personal Data Protection Commissioner provide further guidance on matters including data-breach notification, DPO appointment, cross-border transfers, data protection impact assessments, data protection by design, and automated decision-making and profiling. These instruments are important to the practical operation of the amended statutory framework because they provide more detailed direction on the implementation of data-protection obligations in contemporary data-processing environments.

These reforms are particularly relevant to the digital energy sector. Data-breach notification requirements enhance accountability where security incidents affect personal data, while DPO requirements strengthen organisational oversight of data-processing activities. The statutory right to data portability further strengthens the position of data subjects by enabling them, subject to the requirements of the PDPA, to request the transmission of their personal data from one data controller to another (Personal Data Protection Act 2010, s. 43A).

Nevertheless, the existence of these reforms does not necessarily resolve all privacy concerns associated with digital energy technologies. Smart meters, IoT-enabled devices, AI-based energy-management systems, and interconnected digital platforms may involve continuous and detailed processing of consumer information. Such processing may reveal information about household routines, energy-consumption behaviour, and everyday practices, thereby creating privacy concerns that extend beyond the conventional use of consumption data for billing purposes (Jakobi et al., 2019; Vigurs et al., 2021). The effectiveness of the amended PDPA should therefore be evaluated not only by the existence of statutory rights and obligations but also by their implementation, enforcement, and capacity to address the distinctive characteristics of energy-related consumer data.

The General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR) provides a useful comparative benchmark because it establishes a comprehensive framework governing the processing of personal data and provides extensive rights to data subjects. These include rights relating to access, rectification, erasure, restriction of processing, data portability, objection, and safeguards concerning certain forms of automated decision-making and profiling (Regulation (EU) 2016/679, arts. 15–18, 20–

22). The GDPR also imposes obligations on controllers and processors relating to transparency, accountability, data security, and regulatory compliance.

The GDPR is particularly relevant to the present study because several of its provisions address issues increasingly important in data-driven energy systems. Article 20 establishes the right to data portability, while Article 22 provides safeguards concerning decisions based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects (Regulation (EU) 2016/679, arts. 20, 22). These provisions provide a useful basis for evaluating the extent to which consumers can exercise meaningful control over personal data processed through increasingly automated digital services.

Although recent amendments have brought Malaysia's PDPA closer to contemporary international data-protection practices, the Malaysian and European frameworks should not be treated as identical. Differences remain in their statutory scope, structure of data-subject rights, regulation of automated processing, enforcement mechanisms, and application to particular categories of organisations and processing activities. Accordingly, this study uses the GDPR as a comparative benchmark to identify areas in which Malaysia's post-amendment framework provides protection and areas where further regulatory development may be required, particularly in the digital energy sector.

METHODOLOGY

This study adopts a doctrinal and comparative legal research approach to examine the protection of consumer data and privacy in the digital energy sector. Doctrinal legal research is used to identify, interpret, and analyse the legal rules governing personal data protection in Malaysia, while comparative legal analysis is employed to assess the Malaysian framework against the European Union's General Data Protection Regulation (GDPR). Comparative legal research enables similarities and differences between legal systems to be systematically examined and provides a basis for evaluating alternative regulatory approaches (Eberle, 2011). The analysis draws primarily on legal and regulatory materials relevant to personal data protection. For Malaysia, these include the Personal Data Protection Act 2010 (PDPA), the Personal Data Protection (Amendment) Act 2024, relevant regulations, sector-specific instruments, and guidance issued by the Personal Data Protection Commissioner. The GDPR and relevant European regulatory materials are used as the principal comparative sources. Secondary sources, including journal articles, books, reports, and scholarly commentary, are used to support the interpretation and evaluation of the respective legal frameworks.

The GDPR is selected as the comparative benchmark because it provides a comprehensive data-protection framework and addresses several issues that are increasingly relevant to digital energy systems. The comparison focuses on key areas including the scope of application, consent and transparency, data-subject rights, data portability, data security, data breach notification, automated decision-making and profiling, cross-border data transfers, regulatory enforcement, and sanctions. The analysis further considers how these legal protections operate in the context of digital energy technologies, particularly smart meters, IoT-enabled devices, interconnected energy systems, and AI-based energy-management systems. Particular attention is given to whether the Malaysian framework provides adequate protection against risks arising from continuous data collection, behavioural inference, unauthorised disclosure, cybersecurity threats, and increasingly automated processing of consumer data.

Through this approach, the study identifies areas in which Malaysia's post-amendment PDPA has strengthened consumer data protection, as well as areas where regulatory gaps may remain. The comparison is not intended to suggest that Malaysia should replicate the GDPR in its entirety. Rather, the GDPR is used as a benchmark to evaluate whether additional or sector-specific safeguards may strengthen consumer privacy and data protection within Malaysia's evolving digital energy sector.

FINDINGS AND DISCUSSIONS

Strength and Weaknesses of Digitalising the Energy Sector

The analysis indicates that digitalisation offers significant opportunities to improve the efficiency, sustainability, and responsiveness of the energy sector. Smart meters, IoT-enabled devices, and digital energy-management systems can provide

consumers and energy providers with more detailed information about energy consumption, enabling better monitoring and management of energy use. Nevertheless, these benefits are accompanied by significant privacy and security risks.

Digital energy technologies may involve the continuous collection and processing of detailed consumer information. Smart-meter data, for example, may reveal patterns of household energy consumption that can potentially provide insights into household routines and behaviour. Consequently, concerns arise where consumers have insufficient information about how their data are collected, processed, retained, or shared. These risks become more significant when interconnected systems expose consumer information to unauthorised access or cybersecurity threats (Armoogum & Bassoo, 2019; Saeed et al., 2024).

The findings therefore suggest that consumer protection within the digital energy sector requires more than conventional cybersecurity measures. Effective protection also requires transparency regarding data-processing practices, appropriate safeguards against unauthorised access and disclosure, meaningful opportunities for consumers to exercise their data rights, and adequate accountability mechanisms for organisations processing energy-related consumer information.

Remaining Gaps Between the Post-Amendment PDPA and the GDPR

The comparative analysis indicates that the Personal Data Protection (Amendment) Act 2024 has strengthened Malaysia's data-protection framework and addressed several areas that previously distinguished the PDPA from more comprehensive international frameworks. In particular, developments concerning data portability, data breach notification, Data Protection Officers, security obligations, and penalties have strengthened accountability and consumer protection.

Nevertheless, differences remain between the Malaysian and European frameworks. One significant distinction concerns the scope of application. Malaysia's PDPA principally regulates the processing of personal data in connection with commercial transactions and excludes the Federal and State Governments from its application. The GDPR adopts a broader regulatory structure and provides a more extensive framework of data-subject rights and organisational accountability.

Differences also remain in relation to the structure and extent of individual rights and the regulation of emerging forms of data processing. The GDPR contains detailed provisions concerning erasure, restriction of processing, objection, data portability, and certain forms of automated decision-making and profiling. Although Malaysia's recent reforms have strengthened several areas of data protection, the increasing use of AI, smart meters, IoT devices, and automated energy-management systems raises questions about whether general data-protection rules are sufficiently tailored to the distinctive characteristics of digital energy data.

Accordingly, the findings do not suggest that Malaysia's PDPA is simply “insufficient” or that it should replicate the GDPR. Rather, the analysis indicates that Malaysia's post-amendment framework represents significant progress but may benefit from further sector-specific regulatory development, effective implementation, and enforcement in areas particularly relevant to digital energy technologies.

Regulatory Challenges in the Malaysian Context

The effectiveness of Malaysia's data-protection framework in the digital energy sector depends not only on the content of the legislation but also on its implementation and enforcement. The Personal Data Protection (Amendment) Act 2024 strengthened several statutory obligations, including those relating to data security, data-breach notification, the appointment of Data Protection Officers, and data portability. However, increasingly complex technologies may create new challenges for regulators, energy providers, and consumers.

One particular challenge arises from the interconnected and data-intensive nature of digital energy systems. Smart meters, IoT-enabled devices, cloud services, and AI-based systems may involve multiple parties in the collection, processing, storage, and transfer of consumer information. Detailed energy-consumption data generated by smart-metering systems may raise privacy concerns because such data can reveal information about household activities and everyday practices, while data sharing may also affect consumers' sense of autonomy, choice, and control (Jakobi et al., 2019; Vigurs et al., 2021). This can make it more difficult for consumers to understand who processes their data, for what purposes, and whether the information is subsequently shared or used for additional purposes.

Cross-border data processing may present further challenges where energy-related information is processed through cloud infrastructure or service providers located outside Malaysia. Effective implementation of data-protection requirements is

therefore important for maintaining consumer confidence and facilitating responsible data-sharing practices in increasingly interconnected digital markets (OECD, 2013).

These developments suggest that Malaysia's future regulatory approach should focus not merely on achieving formal similarity with the GDPR but on ensuring that its domestic framework remains responsive to emerging technologies. This is particularly important in the digital energy sector, where technological innovation may develop more rapidly than sector-specific legal and regulatory safeguards.

Recommendations

First, matters affecting the fundamental scope of data protection should be addressed through primary legislation where necessary. In particular, policymakers should consider whether the continuing exclusion of Federal and State Governments creates an appropriate level of protection for personal data processed in public-sector digital-energy initiatives. The PDPA expressly excludes the Federal Government and State Governments from its application (Personal Data Protection Act 2010, s. 3). Because statutory scope determines who is legally subject to the PDPA, any extension of that scope would require legislative intervention rather than guidance alone.

Second, the Utilities Sector (Electricity) Code of Practice should be reviewed and updated as an enforceable sectoral code aligned with the post-amendment PDPA. The existing Code was developed under section 23(1)(b) of the PDPA and applies specifically to the Utilities (Electricity) Sector (Personal Data Protection Commissioner [PDPC], 2016). The revised Code should address smart-meter granularity, IoT ecosystems, retention, secondary use, third-party disclosure, cybersecurity, data portability, automated processing, profiling, privacy by design and impact assessment. Where detailed procedural requirements require binding and uniform application across sectors, subsidiary regulations may be preferable to non-binding guidance.

Third, licensing conditions should be considered for regulated energy providers where the governing energy legislation and licensing framework permit data-governance obligations to be attached to licences. Such conditions could require minimum cybersecurity and privacy controls, auditable data-governance arrangements, incident-management procedures and compliance with the applicable sectoral Code. This would connect data protection directly with the regulatory oversight of energy-service providers.

Fourth, regulatory guidance should continue to support implementation in areas where technological practices evolve rapidly, including data protection impact assessment, data protection by design, privacy notices, automated decision-making and profiling. Guidance is particularly suitable for explaining how statutory principles should be applied to emerging AI-enabled energy services, although guidance should complement rather than replace binding obligations where significant consumer rights are at stake.

Finally, Malaysia should adopt a layered regulatory approach: primary legislation for fundamental rights and statutory scope; subsidiary regulations for detailed mandatory procedures; an updated enforceable Utilities Sector (Electricity) Code for sector-specific obligations; licensing conditions for regulated providers where legally available; and regulatory guidance for implementation and emerging technologies. This combination would avoid relying on a single instrument and would allow consumer protection to develop alongside technological change in the energy sector. Further interdisciplinary research involving regulators, energy providers, consumer organisations and technology specialists should evaluate the effectiveness of these safeguards in practice.

CONCLUSION

The digitalisation of Malaysia's energy sector offers significant opportunities to improve efficiency, sustainability, and consumer participation. At the same time, the increasing use of smart meters, IoT-enabled devices, AI-based energy-management systems, and interconnected digital platforms creates new challenges concerning the collection, processing, security, and use of consumer data.

This study finds that Malaysia's PDPA provides an important legal foundation for protecting personal data in commercial transactions and that the Personal Data Protection (Amendment) Act 2024 has significantly strengthened the country's data-protection framework. The introduction of additional requirements concerning data breach notification, Data Protection

Officers, data portability, security obligations, and regulatory accountability represents substantial progress in addressing contemporary data-protection challenges.

Nevertheless, comparison with the GDPR indicates that differences remain in areas such as statutory scope, the structure of data-subject rights, and safeguards relating to increasingly complex forms of automated data processing. These differences are particularly relevant to the digital energy sector because energy-related technologies may continuously generate detailed information capable of revealing patterns of household behaviour and consumption.

Accordingly, the future development of consumer data protection in Malaysia should not focus solely on reproducing the GDPR. Instead, greater attention should be given to the effective implementation and enforcement of the amended PDPA, sector-specific guidance for digital energy services, transparency and meaningful consumer control, and appropriate governance of emerging technologies such as AI and automated decision-making. These measures would allow Malaysia to support technological innovation in the energy sector while providing stronger and more responsive protection for consumer privacy and personal data.

REFERENCES

1. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, 5(1), 1–25. <https://doi.org/10.51594/csitrj.v5i1.699>
2. Ahmad, T., & Zhang, D. (2021). Using the Internet of Things in smart energy systems and networks. *Sustainable Cities and Society*, 68, 102783. <https://doi.org/10.1016/j.scs.2021.102783>
3. Ahmed, M. M., & Ahmed, A. M. (2023). Citizens' data protection in e-government system. *International Journal of Innovative Computing*, 13(2). <https://doi.org/10.11113/ijic.v13n2.389>
4. Anil, C. B., Sivakrishnan, M., Pranave, M., Joseph, M., Unnikrishnan, G., & Raju, M. (2024). *Privacy and security: A comparative study between privacy and security* [Conference paper]. International Conference on Machine Intelligence in Research and Development 2023, Sree Narayana Gurukulam College of Engineering, Kolenchery, India.
5. Armoogum, S., & Bassoo, V. (2019). Privacy of energy consumption data of a household in a smart grid. In *Smart power distribution systems* (pp. 163–177). Elsevier. <https://doi.org/10.1016/B978-0-12-812154-2.00008-0>
6. Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041. <https://doi.org/10.2307/41409971>
7. Bertino, E. (2016). Data security and privacy: Concepts, approaches, and research directions. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)* (pp. 400–407). IEEE. <https://doi.org/10.1109/COMPSAC.2016.89>
8. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
9. Eberle, E. J. (2011). The methodology of comparative law. *Roger Williams University Law Review*, 16(1), 51–72.
10. Fayayola, O., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in IT: A review of techniques and challenges. *Computer Science & IT Research Journal*, 5(3), 606–615. <https://doi.org/10.51594/csitrj.v5i3.909>
11. George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51–75. <https://doi.org/10.5281/zenodo.10639463>
12. Heffron, R. J., Rønne, A., Tomain, J. P., Bradbrook, A., & Talus, K. (2018). A treatise for energy law. *The Journal of World Energy Law & Business*, 11(1), 34–48. <https://doi.org/10.1093/jwelb/jwx039>
13. Hoang, T. (2024). Impact of integrated artificial intelligence and Internet of Things technologies on smart city transformation. *Journal of Technical Education Science*, 19, 64–73. <https://doi.org/10.54644/jte.2024.1532>
14. Husaini, D. H., & Lean, H. H. (2022). Digitalization and energy sustainability in ASEAN. *Resources, Conservation and Recycling*, 184, 106377. <https://doi.org/10.1016/j.resconrec.2022.106377>
15. Jakobi, T., Patil, S., Randall, D., Stevens, G., & Wulf, V. (2019). It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Transactions on Computer-Human Interaction*, 26(1), 1–44. <https://doi.org/10.1145/3281444>
16. Jenkins, K., McCauley, D., Heffron, R., Stephan, H., & Rehner, R. (2016). Energy justice: A conceptual review. *Energy Research & Social Science*, 11, 174–182. <https://doi.org/10.1016/j.erss.2015.10.004>

17. Kavak, A. (2024). Privacy of information and data: Policies, threats, and solutions. In K. Helge & C. A. Rookey (Eds.), *Creating and sustaining an information governance program* (pp. 155–187). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-0472-3.ch009>
18. Ke, Z., & Yongzhen, L. (2021). Research on Internet data security and privacy protection. *Journal of Physics: Conference Series*, 2005(1), 012004. <https://doi.org/10.1088/1742-6596/2005/1/012004>
19. Montalbano, L. (2021). Transparency in a digitally intertwined world: A hybrid approach to consumers' protection. *Open Journal of Social Sciences*, 9(8), 448–485.
20. Muralidhara, S., Hegde, N., & Rekha, P. M. (2020). An Internet of Things-based smart energy meter for monitoring device-level consumption of energy. *Computers & Electrical Engineering*, 87, 106772. <https://doi.org/10.1016/j.compeleceng.2020.106772>
21. Nageye, A. Y., Jimale, A. D., Abdullahi, M. O., Ahmed, Y. A., & Jama, B. S. A. (2023). Enhancing energy efficiency in Mogadishu: IoT-based buildings energy management system. *SSRG International Journal of Electrical and Electronics Engineering*, 10(10), 54–60. <https://doi.org/10.14445/23488379/IJEEE-V10I10P106>
22. OECD. (2013). Exploring the economics of personal data: A survey of methodologies for measuring monetary value (OECD Digital Economy Papers No. 220). OECD Publishing. <https://doi.org/10.1787/5k486qtxldmq-en>
23. Oprea, S.-V., & Bâra, A. (2024). Generative literature analysis on the rise of prosumers and their influence on the sustainable energy transition. *Utilities Policy*, 90, 101799. <https://doi.org/10.1016/j.jup.2024.101799>
24. Personal Data Protection Commissioner. (2016). Personal data protection code of practice: Utilities sector (electricity). Department of Personal Data Protection, Malaysia.
25. Personal Data Protection Act 2010 (Act 709) (Malaysia).
26. Personal Data Protection (Amendment) Act 2024 (Act A1727) (Malaysia).
27. Personal Data Protection (Amendment) Act 2024 (Appointment of Date of Coming into Operation), P.U. (B) 522 (Malaysia).
28. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
29. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>
30. Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., Zafar Iqbal, S., & Almuhaideb, A. M. (2024). Digital transformation in energy sector: Cybersecurity challenges and implications. *Information*, 15(12), 764. <https://doi.org/10.3390/info15120764>
31. Strycharz, J., & Duivenvoorde, B. (2021). The exploitation of vulnerability through personalised marketing communication: Are consumers protected? *Internet Policy Review*, 10(4), 1–27. <https://doi.org/10.14763/2021.4.1585>
32. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
33. Vigurs, C., Maidment, C., Fell, M., & Shipworth, D. (2021). Customer privacy concerns as a barrier to sharing data about energy use in smart local energy systems: A rapid realist review. *Energies*, 14(5), 1285. <https://doi.org/10.3390/en14051285>
34. Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. *Fundamental Research*, 1(5), 543–551. <https://doi.org/10.1016/j.fmre.2021.08.009>
35. Wang, J., Gao, F., Zhou, Y., Guo, Q., Tan, C.-W., Song, J., & Wang, Y. (2023). Data sharing in energy systems. *Advances in Applied Energy*, 10, 100132. <https://doi.org/10.1016/j.adapen.2023.100132>